# Effective Response to Attacks On Department of Defense Computer Networks

A Monograph
by
Colonel Patrick J. Shaha
Signal

School of Advanced Military Studies
United States Army Command and General Staff College
Fort Leavenworth, Kansas

May 2001

# REPORT DOCUMENTATION PAGE

| 1. REPORT DATE (DD-MM-YYYY) | 2. REPORT TYPE | 3. DATES COVERED (FROM - TO) |
|---|---|---|
| 01-04-2001 | monograph | xx-02-2001 to xx-04-2001 |

| 4. TITLE AND SUBTITLE | 5a. CONTRACT NUMBER |
|---|---|
| Effective Response to Attacks On Department of Defense Computer Networks | 5b. GRANT NUMBER |
| | 5c. PROGRAM ELEMENT NUMBER |
| Unclassified | |
| **6. AUTHOR(S)** | 5d. PROJECT NUMBER |
| Shaha, Patrick J. ; | 5e. TASK NUMBER |
| | 5f. WORK UNIT NUMBER |
| **7. PERFORMING ORGANIZATION NAME AND ADDRESS** | 8. PERFORMING ORGANIZATION REPORT NUMBER |
| U.S. Army Command & General Staff College<br>School of Advanced Military Studies<br>1 Reynolds Ave.<br>Fort Leavenworth , KS 66027 | |
| **9. SPONSORING/MONITORING AGENCY NAME AND ADDRESS** | 10. SPONSOR/MONITOR'S ACRONYM(S) |
| | 11. SPONSOR/MONITOR'S REPORT NUMBER(S) |
| , | |

**12. DISTRIBUTION/AVAILABILITY STATEMENT**

A

PUBLIC RELEASE

,

**13. SUPPLEMENTARY NOTES**

**14. ABSTRACT**

The proliferation of information technology within Department of Defense (DoD) has markedly improved the speed and reach of command and control capabilities. The ease of entry and global availability of network access makes automation linked through networks an optimal medium for sharing information. For the Commanders-in-Chief (CINCs), computer networking has proven especially useful in maintaining contact and sharing data with elements forward deployed as well as with host nation governments and agencies. The significant improvements have come, however, at a high cost in security. Internet access is, by design, wide open to all public networks and to all users, regardless of nationality, language, or intent (criminal or otherwise). Though protection measures are somewhat more robust than in the recent past, virtually any network user is capable of causing serious damage to systems connected to the Internet, as well as trigger isolated collapse of the network itself. The ability to selectively share and deny access to sensitive information with multiple network users has proven a daunting challenge. To date there is no central authoritative body empowered to direct Internet structure or enforce rules of operation. Rather, the very lack of regulation and oversight is seen as the real strength and power of the Internet. Within the regimented world of the DoD there has been in the past little cooperative agreement on how to handle network standardization and upgrade issues, particularly when the warfighting CINCs attempt to use their Title X authority to enhance interoperability among their subordinate service components. Is there relevance for a CINC and his theater to properly respond to a Computer Network Defense (CND) event without an accompanying global response? Does the current chain-of-command for such a response provide the speed and capabilities to assure the security of DoD networks? The current status of CND efforts within DoD supports the conclusion that DoD can effectively implement timely and appropriate responses to detected computer network attacks. Though there remains room for improvements to DoD monitoring and detection capabilities, the positive progress and sense of urgency demonstrated by ongoing efforts forecasts a promising future. Important progress is being made in establishing the sense among the nation?s public and private sector leadership that national security is directly tied to economic security, and that economic security is dependent on the viability and security of the national infrastructures. The monograph makes several recommendations regarding further actions needed to enhance United States capabilities, particularly those of DoD, to deal with the global challenge of CND.

**15. SUBJECT TERMS**

information technology; Computer Network Defense (CND)

| 16. SECURITY CLASSIFICATION OF: | | | 17. LIMITATION OF ABSTRACT | 18. NUMBER OF PAGES | 19a. NAME OF RESPONSIBLE PERSON |
|---|---|---|---|---|---|
| | | | | 51 | Burgess, Ed<br>burgesse@leavenworth.army.mil |
| a. REPORT<br>Unclassified | b. ABSTRACT<br>Unclassified | c. THIS PAGE<br>Unclassified | Same as Report (SAR) | | 19b. TELEPHONE NUMBER<br>International Area Code<br><br>Area Code Telephone Number<br>913 758-3171<br>DSN 585-3171 |

SCHOOL OF ADVANCED MILITARY STUDIES

MONOGRAPH APPROVAL

Colonel Patrick J. Shaha

Title of Monograph: *Effective Response to Attacks On Department of Defense Computer Networks*

Approved by:

_____ Monograph Director
Richard Simon, Chief, LIWA IO Det., CAC

_____ Director, School of Advanced
COL Robin Swan, MMAS Military Studies

_____ Director, Graduate Degree
Robert Berlin, Ph.D. Program

Accepted this 30th Day of April 2001

## ABSTRACT

Effective Response to Attacks On Department of Defense Computer Networks by COL Patrick J. Shaha

The proliferation of information technology within Department of Defense (DoD) has markedly improved the speed and reach of command and control capabilities. The ease of entry and global availability of network access makes automation linked through networks an optimal medium for sharing information. For the Commanders-in-Chief (CINCs), computer networking has proven especially useful in maintaining contact and sharing data with elements forward deployed as well as with host nation governments and agencies.

The significant improvements have come, however, at a high cost in security. Internet access is, by design, wide open to all public networks and to all users, regardless of nationality, language, or intent (criminal or otherwise). Though protection measures are somewhat more robust than in the recent past, virtually any network user is capable of causing serious damage to systems connected to the Internet, as well as trigger isolated collapse of the network itself. The ability to selectively share and deny access to sensitive information with multiple network users has proven a daunting challenge.

To date there is no central authoritative body empowered to direct Internet structure or enforce rules of operation. Rather, the very lack of regulation and oversight is seen as the real strength and power of the Internet. Within the regimented world of the DoD there has been in the past little cooperative agreement on how to handle network standardization and upgrade issues, particularly when the warfighting CINCs attempt to use their Title X authority to enhance interoperability among their subordinate service components. Is there relevance for a CINC and his theater to properly respond to a Computer Network Defense (CND) event without an accompanying global response? Does the current chain-of-command for such a response provide the speed and capabilities to assure the security of DoD networks?

The current status of CND efforts within DoD supports the conclusion that DoD can effectively implement timely and appropriate responses to detected computer network attacks. Though there remains room for improvements to DoD monitoring and detection capabilities, the positive progress and sense of urgency demonstrated by ongoing efforts forecasts a promising future. Important progress is being made in establishing the sense among the nation's public and private sector leadership that national security is directly tied to economic security, and that economic security is dependent on the viability and security of the national infrastructures. The monograph makes several recommendations regarding further actions needed to enhance United States capabilities, particularly those of DoD, to deal with the global challenge of CND.

# TABLE OF CONTENTS

Page

# CHAPTER 1

## Introduction to the Computer Network Defense Situation

> " . . . advances in information technology and competitive pressure to improve efficiency and productivity have created new vulnerabilities to . . . information attacks as these infrastructures have become increasingly automated and interlinked. If we do not implement adequate protective measures, attacks on our critical infrastructures and information systems by nations, groups, or individuals might be capable of significantly harming our military power and economy."[1]
>
> National Security Strategy, October 1998

In the summer of 1997, as part of the Commander-in-Chief (CINC) Pacific (CINCPAC) joint exercise Eligible Receiver, a team of computer experts from the National Security Agency (NSA) (with the mission to break into the CINCPAC computer networks) was included for the first time as part of enemy forces. The attacks were so successful, and so disruptive to the conduct of the exercise that they completely altered Pentagon thinking about cyberwarfare.[2]

The dramatic proliferation of computer networking and interconnectivity experienced over the recent years has revolutionized the way business and government affairs are conducted, as well as the way the global neighborhood communicates. Unlimited numbers of individuals and businesses can now share and exchange information instantaneously on a global scale through Internet Web sites, bulletin boards and electronic mail. The enormous benefits of the information technology revolution are readily available to virtually anyone with access to an inexpensive personal computer and a modem port into the telephone system.

However, the phenomenal benefits of this global interconnectivity carry with them imposing risks from parties who would abuse the open and unregulated nature of the technology, the very thing which makes it so successful. The vulnerability of infrastructures critical to the defense and economic viability of the United States is of particular import to the vital interests of the nation. As the nuclear threat has diminished, new technologies have appeared that have

---

[1] The White House, *A National Security Strategy for a New Century*, October 1998, 20.
[2] Stephen Green, *Pentagon, Once Stung, Beefs Up Cyberwarfare Role*, Copely News Service, December 24, 1999

virtually eliminated the status historically enjoyed by the United States as a sanctuary from foreign aggression. A computer anywhere in the world can now open valves, divert funds, alter switches, or send military orders instantaneously to virtually any point on the globe, traversing undetected through international borders and legal jurisdictions.

The critical infrastructures of energy, telecommunications, transportation, banking and finance, and vital human services (government, emergency services, water, etc.)—including military warfighting capability—rely heavily on the security of their supporting computer operations. As the most advanced nation on earth, the United States is also the most vulnerable—the highest user of computers and automation, the greatest user of electricity. Recent efforts to economize in the commercial sector have often resulted in businesses so tightly reliant on "just-in-time" processes that any disruption could prove catastrophic.

The 1997 Report of the President's Commission on Critical Infrastructure Protection went a long way toward describing the current dilemma facing the nation.

> We found that the nation is so dependent on our infrastructures that we must view them through a national security lens. They are essential to the nation's security, economic health, and social well being. In short, they are the lifelines on which we as a nation depend. We also found the collective dependence on the information and communications infrastructure drives us to seek new understanding about the Information Age. Essentially, we recognize a very real and growing cyber dimension associated with infrastructure assurance. . . . the defenses that served us so well in the past offer little protection from the cyber threat.[3]

The Commission report rightly points out that national defense is no longer exclusively a government issue and that economic security is no longer exclusively a business issue. The rapidly expanding number of computer-literate people, wide distribution of "hacker tool" libraries, and easily obtainable Internet access have only aggravated the risks to legitimate information operations.

[3] *The Report of the President's Commission on Critical Infrastructure Protection*, by Robert T. Marsh, chairman (Washington, D.C., Government Printing Office, 1997), vii.

Deregulation of the public telecommunications network has also aggravated the situation by significantly expanding the number of managers responsible for security as well as the magnitude of access points available to an attacker, each of which may have to be protected. Many new partnership companies involved in the deregulation are significantly foreign owned, further complicating the issue of establishing security and trust relationships and making unauthorized access easier than ever until safeguards can be agreed upon.[4]

Without appropriate safeguards, individuals or organizations may gain unauthorized access to sensitive national systems and cause serious interference and disruption. Whether the damage is inadvertent by authorized computer users, is caused by some natural catastrophe, or is the result of malicious intrusion by parties intent on creating havoc, the results are the same and can have devastating effects on unprotected information and hardware. Potential threats range from the so-called "recreational hackers" to "cyberterrorists" to nation-sponsored information warfare teams. Consistently branded the most potentially damaging threat is the insider, the legitimate user with authorized access to the information system. Recently identified by the Federal Bureau of Investigation (FBI) as the principle source of computer crime, the insider either willingly inflicts damage (e.g. the disgruntled employee), or unwittingly brings destruction on the system (e.g. inserting a disk or file with hidden code, compromising passwords, etc.).

In May, 1998, Stanford Research International (SRI) principal scientist Peter G. Newmann testified before the Senate warning the nation's critical infrastructures are "closely interdependent; a failure on one sector can easily affect other sectors." The implications of this interdependence on Department of Defense (DoD) operations are enormous. In a 1997 Senate hearing Newmann testified:

> Our national infrastructure depends not only on our interconnected information systems and network, but also the public switched network, the air-traffic control systems, the power grids and many associated control systems, which themselves depend heavily on computers and communications. Global problems can result

---

[4] Ibid., A-5.

> from seemingly isolated events, as exhibited by the early power-grid collapses, the 1980 ARPANET collapse and the 1990 long-distance collapse—all of which began with single-point failures. Our defenses against isolated attacks and unanticipated events are inadequate. Risks include not just penetrations and insider misuse, but also insidious Trojan horse attacks that can be dormant until triggered. Our defenses against large-scale coordinated attacks are even more inadequate.[5]

The incentives for such attacks are immense. Trillions of dollars of transactions freely flow over networks that are virtually unprotected and in a medium where legality is largely undefined and very difficult to enforce. Computer crime will continue to grow where strong prosecution is not enforced. Depending on their objectives, attackers may choose to modify, steal or destroy information stored in the system or traversing the network, or to degrade the system to deny access by legitimate users.

A new geography must be dealt with in cyberspace. There are no borders or international boundaries, distance is irrelevant, and attacks can be conducted in near-real time from anywhere with telephonic access to any other point in the global network. Cyberterrorist targets are likely to produce little physical effect, but have the potential for widespread psychological impact. Many targets capable of infrastructure disruption are located in sparsely populated, isolated locations—where physical attack would not result in many casualties or timely notoriety. However, significant psychological stress can be exacted through the disruption of public safety systems, the stealing of intellectual property, tampering with military deployment and reporting networks, which can all be accomplished without warning to the victim, in virtually assured anonymity, and without ever having to confront the military power of the target nation.

Retired U.S. Army Lieutenant General Robert L. Schweitzer, testified before Congress in June, 1998, that:

> The paradigm of war may well be changing. If you can take out the civilian economic infrastructure of a nation, then that nation in addition to not being able

[5] Amara D. Angelica, *The New Face of War*, p. 3; available from http://www.techweek.com/articles/11-2-98/cyper.htm; Internet; accessed 1/5/01.

> to function internally cannot deploy its military by air or sea, or supply them with any real effectiveness—if at all.[6]

On October 6, 1999, in a statement before the Senate Judiciary Committee Subcommittee on Technology and Terrorism, Director of the FBI's National Infrastructure Protection Center (NIPC), Michael A. Vatis, presents a sobering picture of the growing threat. He states the Deputy Secretary of Defense had reported that DoD was detecting 80 to 100 potential hacking events daily, and that FBI computer hacking and network intrusion cases had doubled each year for the past two years. Vatis estimates the damages in the first two quarters of 1999 from viruses[7] alone exceeded $7 billion, and losses by the 163 businesses surveyed by the FBI from computer security breaches were over $123 million. He cites the book published recently by two Chinese military officers that calls for asymmetric measures[8], including cyberattacks through computer viruses, to counter the military might of the United States. Since that time, numerous such attacks have been detected, including the group of Serbian hackers, calling themselves the Black Hand, claiming responsibility for crashing a Kosovo Albanian Web site and threatening attacks on the North Atlantic Treaty Organization (NATO) site. After the Chinese embassy was accidentally bombed in Belgrade, Chinese "hactivists" posted messages such as "We won't stop sending these until the war stops" on U.S. government Web sites. In September, 1999, ten thousand Internet hactivists calling themselves the Electronic Disturbance Theater launched a denial-of-service (DOS) attack against the Pentagon, the Frankfurt Stock Exchange, and the Mexico presidential Web servers to demonstrate solidarity for the Zapatista movement struggles in Chiapas, Mexico.[9]

---

[6] Ibid., p. 5.

[7] A virus is a program or piece of software code that replicates, "infecting" another program, sector or document by inserting itself or attaching itself to that medium. Most just replicate, but some do a lot of other damage.

[8] Qiao Liang and Wang Xiangsui, *Unrestricted Warfare*, Beijing: PLA Literature and Arts Publishing House, February 1999.

[9] Dorthy E. Denning, "Cyberterrorism," (testimony before the U.S. House of Representatives Special Oversight Panel on Terrorism Committee on Armed Services, Washington, D.C., 23 May 2000), available at http://www.terrorism.com/documents/denning-testimony.shtml; Internet, accessed 10/25/00.

According to John Tritak, Director of the Critical Infrastructure Assurance Office (CIAO), Department of Commerce,

> When you're talking about information warfare, you're talking about information systems used to cripple the government and economy. Close to 90% of those critical infrastructure companies are privately owned and operated. . . . The concept of information warfare doesn't present a compelling case to the [Chief Executive Officer] and the board, whose responsibility is to their shareholders and customers. But as they begin to see that operating in a reliable and secure business environment is part of taking full advantage of the Information Age, they get it.[10]

A 1996 survey conducted by the Science Applications International Corporation (SAIC) indicates over $800 million in losses to computer break-ins by the forty corporations polled. Though the incidence of computer break-ins is alarming, even more sobering is the fact that only a miniscule percentage of actual break-ins are ever detected, and only a small number of those detected are reported. The Defense Information Security Agency (DISA), after a series of self-generated attacks on government systems, reports that eighty-eight percent of the 3000 defense computer systems are "easily penetrable." Of the attacks made, ninety-six percent were undetected, and of the four percent detected only five percent were ever reported or investigated by the targeted site.[11]

The lack of emphasis on infrastructure protection has been frustrating. Neumann of SRI thinks it may take a "Chernobyl-scale event" to bring sufficient attention to the issue before a solution can be effected. Following the wakeup call from the summer 1997 Eligible Receiver exercise, however, much progress has been made. In October, 1997, the President's Commission on Critical Infrastructure Protection released its first report calling for a national effort to assure

[10] Deborah Radcliff, "Inforwargames," *Computerworld*, January 22, 2001, 44.
[11] "Statistics on Cyber-terrorism," available from http://www-cs.etsu.edu/gotterbarn/stdntppr/stats.htm; Internet; accessed 1-/25/2000.

the security of the increasingly vulnerable infrastructures upon which the welfare and stability of the nation, and consequently the free world, is so dependent.

The publishing of Presidential Decision Directive 63 (PDD-63) in May, 1998, has been vital to galvanizing the efforts of commercial interests and government agencies in meeting the Commission's recommendations to protect the increasingly exposed and interdependent national information infrastructures. PDD-63 is the result of an extensive interagency effort to evaluate the Commission's recommendations and create a workable plan to establish effective critical infrastructure protection mechanisms against both physical and cyber attacks. Among other things, policy set forth in PDD-63 calls for:

- a reliable, interconnected, secure information infrastructure by the year 2000
- establishment of a national center to warn of and respond to attacks on the information infrastructure
- building the capability to protect critical infrastructures from intentional attacks by 2003
- federal departments and agencies will work to reduce exposure to cyber threats
- the federal government serving as the model to the rest of the nation for how infrastructure protection is to be attained.[12]

Of particular interest is the impact of CND on national defense. Failure to protect the flow of defense information could determine battlefield results, not to mention the ability to even deploy to the battlefield. US Air Force General Ralph E. Eberhart, Commander-in-Chief (CinC), USSPACECOM, has stated "Joint Vision 2010 [and a recently updated version, Joint Vision 2020] recognizes information superiority as the key enabler to achieve the goal of a joint force that is dominant across the full spectrum of military operations—persuasive in peace, decisive in war, and preeminent in any form of conflict. Effective global computer network defense operations are essential to information superiority."[13]

---

[12] The White House, *White Paper: Protecting America's Critical Infrastructures, PDD-63*, Office of the Press Secretary, May 22, 1998, available from http://www.info-sec.com/ciao/63factsheet.html; Internet, accessed 25/10/00.

[13] John Roos, "USSPACECOM Readies For Computer Network Attack Mission," *Armed Forces Journal International*, 2 October 2000, 2.

Ongoing DoD efforts toward ensuring information and network security have only intensified as a result of PDD-63. The monograph will examine whether the current system for responding to attacks within the DoD computer networks can effectively orchestrate appropriate, timely, coordinated, global reaction measures. Though the research topic seeks to determine DoD readiness in dealing with CND, much attention must be paid to the federal government agencies and activities that establish strategic policy and enforce national directives in the pursuit of the security of the nation's information infrastructure. A description of the U.S. system for CND, to include the DoD system, will be followed by a discussion of the requirements and standards for effective CND using the latest technologies. The research question will be answered based upon DoD's ability to meet the current threat through incorporation of the latest advances in technology and procedure.

## CHAPTER 2
### U.S. Computer Network Defense Response Systems

Since the issuance of PDD-63, significant progress has been made in establishing a federal system to deal with U.S. computer and network vulnerabilities. The system of centers and automated sensor and reporting capabilities has become extensive, even cumbersome, and has endeavored to incorporate all government agencies and elements along with the major commercial and private users of the nations critical infrastructures. To succeed in eliminating potential weaknesses and in responding effectively to attack, a concerted and cooperative partnership is deemed vital in establishing procedures and activities for mutual protection.

PDD-63 calls for breaking down the nation's critical infrastructures into sectors, assigning a government agency to act as lead agency for each, and calling for a senior official from the lead agency to act as the Sector Liaison Official. Each of the officials, in coordination with the private sector entities within the sector, identifies a counterpart from the private sector to represent the interests of the sector entities. The two individuals, along with the departments and corporations they represent, establish and implement a plan meant to accomplish the following:

- assess the sector vulnerabilities to cyber attack
- recommend a plan to eliminate significant vulnerabilities
- propose a system for identifying and preventing major attacks
- develop a plan for alerting, containing and responding to an attack in progress and rapidly reconstitute minimum essential capabilities.[14]

Provision is made also for a National Coordinator who, among other responsibilities, ensures the sector plans for the various critical infrastructures are coordinated, with particular emphasis on interdependencies.

In addition to the critical infrastructures, PDD-63 assigns several government agencies as lead elements for protecting certain critical functions related to the protection of the

[14] The White House, *PDD63: White Paper on Administration's Policy on Critical Infrastructure Protection*, Office of the Press Secretary, May 1998, available from http://www.ciao.gov/CIAO_Document_Library/paper598.pdf; Internet, accessed 25/10/00.

infrastructures, protection primarily performed by the federal government, i.e. national defense, foreign affairs, intelligence, and law enforcement. Each lead agency appoints a Functional Coordinator, to be of Assistant Secretary rank or higher, responsible for coordinating all government activities in that functional area. PDD-63 assigns lead agency accountability within the U.S. Government for the specific infrastructure sectors and functions are as follows:

| **Lead Agency** | **Sector** |
|---|---|
| Commerce | Information and communications |
| Treasury | Banking and finance |
| Environmental Protection Agency | Water supply |
| Transportation | Aviation, Highways, Mass transit, Pipelines, Rail, Waterborne commerce |
| Justice/Federal Bureau of Investigation | Emergency law enforcement services |
| Federal Emergency Management Agency | Emergency fire service<br>Continuity of government services |
| Health and Human Services | Public health services |
| Energy | Electric power, Oil and gas production and storage |
| **Lead Agency** | **Special Function** |
| Justice/FBI | Law enforcement and internal security |
| Central Intelligence Agency | Foreign intelligence |
| State | Foreign affairs |
| Defense | National defense |

Despite the Department of Commerce being assigned lead for information and communications, the Department of Defense retains Executive Agent responsibility for the National Communications System.

To ensure coordination of effort among the sectors and functional areas, PDD-63 provides for a Critical Infrastructure Coordination Group (CICG) where all the coordinators, as well as representatives from other relevant departments and agencies, meet to implement the Directive. The CICG is chaired by the National Coordinator who is appointed by and reports to the President through his Assistant for National Security Affairs.

On 14 July 1999, by Executive Order, President Clinton established the National Infrastructure Assurance Council (NIAC) to advise the President on cybersecurity and to enhance the cooperative partnership between public and private sectors in addressing the threat to the computer and networking services upon which the nation depends daily. One of the biggest duties of the NIAC is to monitor the development of the private sector Information Sharing and Analysis Centers (ISAC), called for in PDD-63 as the liaison between the National Infrastructure Protection Center (NIPC) and the various critical infrastructure sectors. The NIPC is located at the FBI headquarters in Washington, D.C. and is a joint government and private sector partnership with the mission to address the protection of national critical infrastructures, focusing primarily on computer-connected criminal activity. The most recent addition to the list of ISACs was the January 2001 establishment of the Information Technology ISAC.[15]

The move by President Clinton to make several key last-minute appointments to the NIAC prior to his leaving office has called its viability into question. Clinton's former senior director for Critical Infrastructure Protection at the National Security Council (NSC), Jeffrey Hunker, said the key element of the protection effort was created "explicitly recognizing that this was a new type of challenge and that a czar-like structure would not work. There are too many interests and powerful interests involved . . . . Still, you need somebody to manage the effort and crack the whip."[16] The executive order creating the NIAC expires at the end of two years and the new administration may just allow it to run out and the Council to dissolve. There are those,

[15] John Roos, 5.
[16] Dan Verton, "Clinton makes last-minute cybersecurity appointments," Computerworld, 22 January 2001.

however, that feel the NIAC function will be important in orchestrating the success of ongoing efforts at infrastructure protection and will hopefully survive the change in administrations.[17]

PDD-63 directs the establishment of national warning and information sharing systems. Mentioned briefly earlier, the primary center for coordination of national warning and information sharing is the FBI's National Infrastructure Protection Center (NIPC). According to the NIPC Director, Michael Vatis, the center was created in 1998 as the focal point of U.S. government efforts to warn of and respond to cyber intrusions.[18] To perform this vital mission, the NIPC establishes working relationships with a wide range of activities, both government and private sector. Secret Service, FBI, and other representatives experienced in computer crime and infrastructure protection work at the NIPC, along with representatives from the other lead agencies and the intelligence community. Electronic links provide for the constant sharing of information and the issuance and exchange of timely warnings via a secure alert network called Infraguard.

Being an element of the FBI, with an understandable focus on law enforcement, the NIPC is somewhat hindered in it's ability to provide effective oversight of information infrastructure warning and response mechanisms. The new presidential administration could bring a major change to the government structure and procedures for reacting to cyberattack. Some discussion has already centered on the possibility of designating an Information Technology (IT) Czar to establish firmer structure and more effective management of national IT resources and investments. Such a move would likely cause a restructuring of the detection and response system in place, and possible change the role of the NIPC. Support for such a move is basically

[17] President, Executive Order 13130, "National Infrastructure Assurance Council," available at http://cio.gov/docs/eo13130.htm; Internet, accessed 1/25/01.
[18] Michael A. Vatis, "NIPC Cyber Threat Assessment, October 1999" (statement for the record before the Senate Judiciary Committee Subcommittee on Technology and Terrorism, Washington, D.C., 6 October 1999), available from http://www.fas.org/irp/congress/1999_hr/nipc10-6.htm; Internet, accessed 10/25/00. Vatis quotes the NIPC mission as directed by PDD-63 as to "serve as a national critical infrastructure threat assessment, warning, vulnerability, and law enforcement investigation and response entity."

driven by the NIPC's inability to freely communicate information on cyberattacks in a timely manner (due to privacy restrictions) while having to treat such attacks as law enforcement investigations. Confusion results when some question the delays from what they see as a national detection and warning center, while others go elsewhere for information and support because they see NIPC as a law enforcement agency.[19]

To facilitate the FBI's ability to investigate and respond to cyber attacks, the Bureau has created in each of its fifty-six field offices a National Infrastructure Protection and Computer Intrusion (NIPCI) element. To deal with the exceptionally difficult issue of cybercrime, the Justice Department recently established an Internet Web site to consolidate information on the growing problem.[20]

In response to PDD-63, many other government departments and agencies have also formed some type of element to deal with the cyber threat. The Office of Management and Budget (OMB) is responsible for managing vulnerability and risk assessments for federal agencies, and for incorporating infrastructure protection into their reporting systems (also required by OMB Circular A-130). To manage the federal government's civilian computer protection activies, the General Services Administration (GSA) established the Federal Computer Incident Response Center (FedCIRC) to provide a central focal point for government computer incident reporting, handling, prevention and recognition. FedCIRC is a collaborative partnership of computer and law enforcement professionals providing both proactive and reactive security services for federal government computers and networks.[21]

The energy infrastructure sector, composed of increasingly interdependent industries that produce and distribute electric power, oil, and natural gas, is exceptionally reliant on computer control of power grids, pipelines, nuclear facilities and waste sites, etc. The Department of

[19] Dan Verton, "Bush Eyes Overhaul of Nation's E-security," *Computerworld*, 19 December 2000.
[20] "U.S. Launches Cybercrime Web Site," *Reuters*, 3 October 2000
[21] Information on FedCIRC can be accessed on the homepage at http://www.fedcirc.gov.

Energy (DoE), lead agency for the energy sector, established in October 1999 the Office of Critical Infrastructure Protection (OCIP) to develop the capability to protect the nation's critical energy infrastructures in cooperation with domestic, friendly nation, international and multinational corporations and energy interests. The DoE created the Computer Incident Advisory Committee (CIAC) to provide computer security information to DoE employees and contractors. The CIAC's extensive and verifiable listings of server vulnerabilities, Internet hoaxes and chain mail issues are of great valuable to DoE administrators, but are also of extreme value to the common user since the listings are posted on a public access Web site. Unfortunately, reflecting the general state of cyber administration, as of February 1999, only twenty of the seventy-two major energy sector sites and facilities report computer security incidents, and of the twenty only two report all incidents (excluding viruses). However, the number of reports received markedly increases each year.[22]

Moving from the non-military government agencies, DoD has also done much in response to PDD-63 to enhance its capabilities to deal with the cyber threat. Lessons learned from the 1997 Exercise Eligible Receiver debacle, coupled with intensified automation activities associated with the year 2000 (Y2K), resulted in the June 1999 creation of the Joint Task Force for Computer Network Defense (JTF-CND) with responsibility for all DoD computer network defense (CND) and attack (CNA) actions. Since the beginning of fiscal year 2000 the task force has been under the U.S. Space Command (USSPACECOM). The action is a clear signal that the U.S. intends to maintain its historical advantage over all potential adversaries in this vital discipline that will hereafter be handled as a potential arena for warfare. It is DoD's response to the threat of attacks which the most insignificant foe can now easily press against a superpower with virtually no fear of detection or having to face any physical forces.[23]

---

[22] Department of Energy, *Critical Infrastructure Protection Program Related to Cyber Protection* (Washington, D.C., 1999); available from http://www-it.hr.doe.gov/imcouncil/meetings/feb17-19_1999/read_crit.htm; Internet, accessed 02/14/01.

[23] Stephen Green, Pentagon, Once Stung, Beefs Up Cyberwarfare Role," *Copley News Service*, 24

DoD Directive O-8530.1, "Computer Network Defense (CND)," encompasses all DoD components and defines the mission, policy "and responsibilities for essential structure and support to CINC USSPACECOM (USCINCSPACE) for CND within DoD information systems and computer networks."[24] The Directive establishes the policy that all DoD information systems and computer networks will be monitored to "detect, isolate, and react to intrusions, disruption of services, or other incidents that threaten the security or function of DoD operations." Such activities are to include regular and proactive vulnerability analysis and assessment, active penetration testing and implementation of any improvements identified. CND activities are to be coordinated with all federal agencies including law enforcement, intelligence, counterintelligence, as well as with network and information system owners and users.

The Chairman, Joint Chiefs of Staff (CJCS), coordinates with USCINCSPACE to ensure effective CND planning and execution and oversees DoD participation in the NIPC, making sure DoD interests are considered in operations there. The CJCS also requires the Defense Information Systems Agency (DISA) to serve as the technical advisor for CND to the Secretary of Defense, the CJCS, and USCINCSPACE. As the overall integrator of CND systems within DoD, DISA is also tasked with implementing advisory and alert procedures for service providers and with technical alert support for USCINCSPACE release to network operators.[25]

The Directive assigns USCINCSPACE as the lead activity for all DoD CND mission operations, responsible for directing and coordinating any CND operations that impact more than one DoD component. The CINC exercises combatant command authority to plan and execute operations to defend DoD computer networks against any unauthorized intrusion or attack. The CINC is charged with coordinating the release and distribution of CND advisories and alerts and monitoring compliance, activities generally conducted by DISA as the CINC's technical advisor

---

December 1999.
[24] Department of Defense, *DoD Directive 8530.1 Computer Network Defense (CND)*, (Washington, D.C., 2001), 1.
[25] Ibid, 5.

which will be discussed later. The CINC also provides defense-wide situational awareness and attack warning through constantly updated information on the CND Common Operational Picture (CND COP).[26] USCINCSPACE is also responsible for directing changes to the DoD posture of Information Operations Condition (INFOCON), a system in the process of being revised to include a guide to commanders on how to determine an appropriate INFOCON level, actions to be taken at each level, and a standardized reporting process.[27]

Before describing what DoD has created to establish and maintain superiority on the information infrastructure, the concept of the Defense Information Infrastructure should be understood. The web of communications networks, computers, software, databases, applications, weapon systems interfaces, data, security services, and other services that process and transport DoD information, across the range of military operations, is collectively designated the Defense Information Infrastructure (DII). Once fully implemented, the DII will operate as a collection of distributed, heterogeneous and interoperable information systems. It will encompass the entire spectrum of DoD operations, from strategic to sustaining base to tactical levels. The DII implements the vision of command, control, communications, computer and intelligence for the warrior (C4IFTW), providing warfighters and other DoD users the ability to rapidly and securely share information from any location at any time. It is established and administered by DISA in consultation with the CINCs, Services, and other Agencies which identify requirements, both current and future.[28]

DISA, as central manager of the DII, and in coordination with the National Security Agency (NSA), defines information assurance requirements and implementation strategies for the DII. Information assurance (IA) is defined as the operations conducted to protect and defend

---

[26] Ibid, 7.
[27] USDEPCINCSPACE Peterson AFB CO message, Subject: Review of Revised DoD Information Operations Condition (INFOCON) Sytem Procedures, DTG 012106Z FEB 01
[28] Information on the Defense Information Systems Agency was obtained from a series of fact sheets available from the DISA homepage; available from http://www.disa.mil/cmd/pao04.html; accessed 01/18/01.

information and information systems by ensuring their availability, integrity, confidentiality, and authentication as well as providing for their restoration through protection, detection, and reaction capabilities. DISA's IA Program Management Office (IPMO) oversees the acquisition, implementation, integration, and dissemination of IA products and services for DoD systems and activities and is the proponent for IA initiatives with allies and multinational defense organizations (e.g. NATO). The IPMO consolidates requirements from the Joint Staff, CINCs, Services and Agencies, and the intelligence community and establishes standards for IA tools, procedures, and training.

DISA's Operations Directorate manages the DII 24 hours a day, 7 days a week, through the Global Network Operations and Security Center (GNOSC). The GNOSC is responsible for managing, by exception, all network faults or outages that occur anywhere in the DII. Global management is exercised through five subordinate Regional Network Operations and Security Centers (RNOSC). Computer and computer network issues are worked closely with and referred appropriately to the JTF-CND at USSPACECOM and to DISA's DoD Computer Emergency Response Team (DoD-CERT).

The DoD-CERT mission is to protect, defend, and restore the integrity and availability of the essential elements and applications of the DII. It is responsible for global DII intrusion detection, vulnerability analysis and management, and investigation of incidents. In carrying out its duties, the DoD-CERT works in close coordination with the JTF-CND, the RNOSCs and their associated Regional CERTs (RCERT), law enforcement agencies (LEA), intelligence agencies, the Service CERTs, and the Joint Staff. The DoD-CERT staff also provides timely and accurate strategic CND analysis and technical decision making support to the JTF-CND. The DoD-CERT disseminates Information Assurance Vulnerability Assessments (IAVAs) to notify DII points of contact of severe vulnerabilities requiring immediate corrective action. Bulletins (IAVBs) are published when the threat is not immediate but significant enough that non-compliance with the

corrective action could escalate the threat, and Technical Advisories go out when the vulnerability exists but is considered low risk. The DoD-CERT staff provides continuous 24-hour support to resolve any computer incident security problem encountered by DoD elements, and coordinates with the vendor community all technical efforts to develop and disseminate software fixes.

Each Service has also established a computer incident response capability to provide IA to their subordinate elements: the Army's ACERT, the Air Force's AFCERT, and the Navy's NAVCIRT (Computer Incident Response Team) which also serves Marine Corps requirements. Each element provides its respective Service with expert support in the various aspects of CND. Some of the assistance provided includes non-destructive exploitation and "attack" of command information systems to determine vulnerabilities, to raise security awareness, and to train system administrators how to recognize computer network attacks. The expert teams assist Service development of prototype automation and network systems along with concurrent development of accompanying tactics, plans and policies. They provide subject matter expertise in all elements of Information Operations (IO), and support deliberate and crisis planning actions for exercises as well as contingency operations from strategic planning to tactical execution.

In response to a particularly significant Internet outage in 1988[29], DoD has funded the Computer Emergency Response Team/Coordination Center (CERT/CC) as an element of the Software Engineering Institute (SEI) at Carnegie Mellon University. The activity has been and continues to be a vital element in the effective monitoring and detection of Internet-related incidents and alerting of Internet subscribers, both public and private sector, of appropriate actions and responses to incidents. The Center is a key source of technical advisory and

[29] The CERT/CC was started by DARPA (the Defense Advanced Research Projects Agency, part of the DoD) in December 1988 after the Morris Worm incident crippled 10% of all computers connected to the Internet. A worm is a program that makes copies of itself, for example from one disk drive to another, or by copying itself using e-mail or some other transport mechanism.

procedural support to the regional and Service CERTs, and is tasked with technical advisory responsibilities to the JTF-CND.[30]

The DoD response teams react to reports submitted from subordinate IA elements. The GNOSC provides the guidelines for submission of computer and network intrusion reports. Some of the subordinate elements (such as the Service CERTs) have expanded the detail of the guidelines within their areas of purview as necessary. It is instructive to review the information and direction provided in the guidelines.

1. Any user noticing anomalous or suspicious activity will report the situation to the local control centers **immediately**.
2. Events/incidents that fall into one of the following categories are to be reported to the DISA GNOSC through Service and Regional channels:
   a. **Category 1** (GNOSC should receive report within 2 hours of incident)—any incident report that will generate DoD-wide advisories and cause implementation of defensive response measures.
   b. **Category 2** (GNOSC should receive report within 24 hours)—to support ongoing analysis and correlation between incidents/events, or heighten awareness throughout the community
      (1) any unusual system performance or behavior
      (2) system crashes or component outages of a suspicious nature
      (3) abnormal delay in network or application services
      (4) installation of unauthorized software
      (5) missing data, files, or programs
      (6) unexplained access privilege changes
      (7) routine malicious logic (virus) events
      (8) poor security practices (unusual after-hour system activity, unauthorized user privilege activity, etc.)
3. All DoD agencies and other joint activities will report incidents or events affecting collateral networks directly to the DISA GNOSC.
4. Organizations at all levels will provide status reports to the appropriate elements when:
   a. There are increases, decreases, or changes in the nature of an event or incident activity
   b. Corrective actions are taken that change the status of the event or incident activity
   c. A reportable incident or event has been declared closed.[31]

The DISA reporting guidelines go on to provide guidance on approved reporting methods. Reports are to be submitted via the most protected means available for the affected

[30] Information gleaned from CERT/CC homepage, available at http://www.cert.org; Internet, accessed 10/25/2000
[31] Defense Information Systems Agency, *DISA Network Incident Reporting Guidelines*, available from

system; the affected system is not to be used for reporting. Unclassified means are to be used only for initial reports and for a short period immediately following the incident to alert the chain of command that a problem has occurred. Follow-on reports are to be submitted through a secure channel, including: the Secret Internet Protocol (IP) Router Network (SIPRNET), the AUTODIN record message system or its Defense Message System (DMS) replacement, secure facsimile, Secure Telephone Unit (STU-III), and the Defense Red Switch Network (DRSN).

The guidelines specify what information is to be included in the incident report. After identifying itself in the header, the reporting agency must decide what addressees are appropriate (Service CERT/CIRT, CINC and his supporting RNOSC, other commands as necessary, DISA GNOSC, etc.). The report must specify the date and time of the incident, in Zulu time, and provide a narrative description of the incident or event along with any identifiers or serial numbers assigned by the reporting command. The report is to identify the asset that was affected and to describe the impact to the affected system, networks, and information. Further technical details of the incident must identify:

1. Who is the apparent source of the attack (IP addresses, names, etc.)
2. What actually happened
3. When it happened and whether the event is ongoing
4. Where the event was apparently targeting (IP address, names, classification level of the systems affected, etc.)
5. Why (if possible) the attacker apparently targeted the asset and why it was successful (e.g. poor security practices, exploitation of a known vulnerability, etc.)
6. How the incident was caused, if known.

The report is to conclude with a description of all actions that have been taken in response to the incident and information on points of contact at the reporting headquarters and any elements that have been in coordination regarding the incident.

The ACERT has published a very helpful and self-explanatory set of procedures for handling actions in response to an incident/intrusion. The immediate actions prescribed by the

---

http://www.cert.mil/pub/info/general/network.security/reportguidelines/pdf; Internet, accessed 02/22/01.

ACERT to be taken by systems administrators are intended to contain the event and preclude any further damage:

**Do:**
- disconnect the system from the network
- perform a complete system backup to tape or CD
- confirm the integrity of the system backup and place it in a restricted access location
- complete the report format and notify the RCERT and your local Criminal Investigation Division (CID)
- disable associated user accounts, if known, until CID determines the investigative status

**Don't:**
- turn the system off or reboot the computer
- finger or attempt to contact the source of the event directly
- alter or change the system files on the suspicious system
- connect to the system over the network
- allow access to the system by any suspected individuals.[32]

The ACERT report format then prompts the reporting element to fill in the blanks to meet all the DISA requirements, requesting information on hardware nomenclature and installed software, web server public accessibility, network intrusion protection, etc. The ACERT goes on to ask about the latest vulnerability assessment of the system as well as any follow-on actions taken and their results. As part of the report, the ACERT includes guidelines on how to ensure the servicing RCERT has a uniform understanding of the terminology used in the report. The definition provided for the term "incident" is given as:

> **Incident**--The act of violating an explicit or implied security policy. Lacking the implementation of policy, an incident consists of:
> - attempts (failed or successful) to gain unauthorized access to a system or it's data
> - unwanted disruption or denial of service (DOS)[33]
> - unauthorized use of a system for the processing or storage of data
> - changes to system hardware, firmware, or software characteristics without the owner's knowledge, instruction, or consent
> - anomalous activity detected by the IDS [defined in chapter 3].

[32] Army Computer Emergency Response Team, *Procedures for Incident/Intrusion Handling*, electronic mail attachment received 16 February 2001 from Richard Simon, Chief, Land Information Warfare Activity Detachment, Fort Leavenworth, KS.

[33] Denial-of-service attacks flood networks with huge numbers of bogus information requests which can eventually overload the servers and cause them to stop responding to legitimate queries. Mechanisms for stopping such attacks once launched are currently inadequate.

An intrusion is defined as the successful unauthorized access of a system. Though the core of individuals involved in investigating and reporting the incident is small, the effort to fully respond to the event or incident and correct the vulnerabilities exposed should involve the entire agency's management structures, communications elements and users.

Incident reporting mechanisms are constantly being improved and upgraded. The DISA Trouble Management System (TMS), incorporated into the Internet Network Management System (INMS), links the GNOSC with the RNOSCs for immediate sharing of information. Future INMS/TMS service is to be expanded to include the Service CERT/CIRT activities and the local control centers (LCCs).[34]

Another innovation is the upcoming "Do It Yourself Vulnerability Assessment Program," or DITY VAP. Produced by the ACERT, the DITY VAP is designed to provide Army Commands and Activities with the capability to enhance their AI system security through an organic self-assessment tool. The program provides a self-contained library of system assessment tools, along with the requisite training and technical support. It is just one more effort to push security awareness down to appropriate levels, to reduce the need for top-driven network scans across the infrastructure, and to better disseminate methods, techniques and configuration modifications that can enhance network security. As the ACERT transitions to the new program, authorization to scan beyond an Army security device will be restricted, and only the CERT will be allowed to conduct remote scans.[35]

The Services and Agencies continue to improve their network security systems as well. Speaking to the Information Assurance Conference held on September 12, 2000, in Crystal City, Virginia, Lieutenant General Peter M. Cuviello, Department of the Army's (DA) Chief Information Officer (CIO) and Director of Information Systems and Command, Control, Communications and Computers (DISC4), described some significant progress the Army has

[34] Defense Information Systems Agency, *DISA Network Incident Reporting Guidelines*, op. Cit.

made. He outlined several of the more recent successes of the Army's network security improvement programs and announced the expansion of the CERT structure within the Army to include four regional CERTs, located in Europe, Hawaii, Korea and the continental U.S., with the ACERT continuing to operate from Fort Belvoir, Virginia.[36]

LTG Cuviello noted that all Army authorized Non-secure IP Network (NIPRNET) gateway circuits are now protected with IDS equipment that is centrally configured and monitored. The Army has identified and secured 817 critical network servers, which are actively monitored round the clock. The Army trains 2800 military, DA civilians, and contractors serving as network managers each year at twelve different locations worldwide—a major improvement when considering the Army was able to train only 240 at Fort Gordon during the whole of 1998. An additional 300 managers receive specialized training on the IDS and firewall systems protecting the networks, and mobile training teams (MTT) are deployed regularly worldwide to provide IA training and instruction to another 600 enlisted, officer and civilian workers.

---

[35] John Dolak, *DITY VAP*, RCERT-CONUS electronic mail released 24 January 2001.
[36] LTG Peter M. Cuviello, *Information Assurance Readiness Review and IA Force Protection Program Assessment,"* speech delivered to Information Assurance Conference on 12 September 2000, available from http://www.army.mil/disc4/references/Briefings_Cuviello/iaspeech.pdf; Internet, accessed 02/22/01.

## CHAPTER 3

### Computer Network Defense Challenges and Standards

> Ninety percent of our military communications now passes over public networks. If an electromagnetic pulse takes out the telephone systems, we are in deep double trouble because our military and non-military nets are virtually inseparable. It is almost equally impossible to distinguish between the U.S. national telecommunications network and the global one. What this means is that it is finally becoming possible to do what Sun Tzu wrote about 2,000 years ago: to conquer an enemy without fighting.[37]
>
> Robert L. Schweitzer, LTG(R), USA

LTG Cuviello noted in his address that, in spite of all the efforts in security enhancements and training, the number of computer and network incidents and reportable events continues to rise. Since the CERT/CC began tracking incident reports in late 1989, their statistics reveal an alarming and steady increase in the number of incidents and vulnerabilities reported:

| **Year** | **1989** | **1990** | **1993** | **1995** | **1998** | **1999** | **2000** |
|---|---|---|---|---|---|---|---|
| **Incidents** | 132 | 252 | 1334 | 2412 | 3734 | 9859 | 21,756 |
| **Vulnerabilities** | | | 171 | 262 | 417 | 744[38] | |

Over the same time period there has also been a steady increase in the number of security alerts and advisories, as well as vendor bulletins notifying users of potentially hazardous "backdoors" and other software "holes" susceptible to hacker intrusions.

The accelerated increase between 1998 and 2000 is of special concern. LTG Cuviello wondered in his speech whether these increases are the result of an expanding threat or just indicate that system users and administrators are getting better at identifying incidents. He rightly answers his own question in the affirmative on both counts, that there was a time "when we didn't know what we didn't know. And I suppose that will never change. But we know more today."

Though DoD computer protection activities are better today than ever before, unfortunately so are the skills and tools available to those actively seeking unauthorized entry into

---

[37] Angelica, op. Cit., p. 5.

[38] Carnegie Mellon Software Engineering Institute, *CERT/CC Statistics 1988-2000*, available from http://www.cert.org/stats/cert_stats/html; Internet, accessed 2/24/01.

DoD systems. Although there are many highly skilled hackers working to gain access, there is a much higher number of "script kiddies" with ready access to widely available and user friendly "point-and-click" software tools designed to empower the least skilled with some of the most dangerous and effective hacking capabilities. The tools are available for download and execution, and some of the more experienced users can even modify the tools, making intrusion detection and damage repair even more challenging.

The IA alert process is intended to counter these threats. Within DoD directive authority (DoDD O-8530.1) backs the alerts, bulletins, and technical advisories and requires acknowledgment of receipt and dissemination to subordinate elements. Alerts within DoD require compliance and reporting of progress in implementation. However, the guidelines and procedures provided by the centers for emergency computer incident response in the other federal departments and agencies, for example the NIPC, are purely for coordination and advice—no directive authority over the federal agencies, including any civilian direction to DoD, is apparent in the documentation. The new FY 2001 Defense Authorization Act (Public Law 106-389), which includes Title X, subtitle G, "Government Information Security Reform," requires annual agency program reviews and Inspector General evaluations, and the submission of a report annually to OMB as part of the budget process. Yet the Act does not provide any directive authority within the federal agencies and clearly indicates that any actions to enhance information systems security are incumbent on the individual agencies.[39]

The approach taken by DoD is to make it a command concern and direct the establishment of an organization to accomplish the mission. As early as mid-year 2000, Army policy recognized the need for a hierarchy assigned to ensure computer network security and provide information assurance, empowered to enforce whatever actions are necessary to protect vital information infrastructures. In a June 2, 2000 message, the Secretary of the Army

[39] Jack Lew, *Guidance on Implementing the Government Information Security Reform Act*, memorandum dated 16 January 2001

announced an interim policy for the structure for information system security personnel. Under the direction of the Army CIO (Director, DISC4), command IA personnel become the focal point for all IA matters within their commands or activities. They are empowered with the authority to "enforce security policies and safeguards for information systems and information based systems (weapon systems) within their purview. This authority includes recommending halting system operations to the commander if warranted by the impact of a security deficiency."[40]

DoD elements have obvious advantages in exercising authority within a very structured chain of command. However, the approach is instructive when compared to the lack of directive authority exercised by counterpart federal departments and agencies, including elements meant to oversee the protection of vital national infrastructures. FedCIRC circulars "request" department and agency support, give "guidance," and "encourage" interagency cooperation. There does not appear to be anyone in charge of interagency CND efforts, no element empowered to set and enforce authoritative standards for intrusions monitoring, detection and response or for software and hardware systems configuration.

The federal government's conscious decision against regulating private sector compliance in upgrading network security capabilities is sound; no need to alienate the private sector with dictates that are unenforceable anyway. The need for protecting the national information infrastructure creates a shared zone of responsibility between the public and private sectors, and requires cooperation between industry and government to forge a working partnership that can strengthen the viability of the infrastructure without stifling free enterprise. Commercial entities, once apprised of the dangers computer intrusion issues pose to their economic well being, will hopefully wisely invest in the latest protection measures.

However, just as there are provisions for DoD elements to exercise limited command and control authority in some domestic emergency situations (e.g. disaster relief operations), lead

[40] Department of the Army message (SAIS-IAS), date-time group 020919Z Jun 00, Subject: New Information Assurance (IA) Personnel Structure.

federal activities should have the power to impose compliance with minimal computer and network security measures when indicated by the interests of national security. For example, the issue of computer security in municipal communities may appear to be strategically unimportant, but national interests quickly come into play when a determined enemy can hack into a city computer system and shut down or alter airfield or port operations and delay, or even terminate, a military deployment. And for all their computer and network protection capabilities and intentions, NIPC and FedCIRC attentions are primarily directed toward handling ongoing criminal and multi-agency computer issues, with limited potential for much of a proactive or reactive role in handling actual incidents. Any help in the latter areas is most likely to be expected to come from the JTF-CND. But with JTF-CND now spearheading DoD CND activities and focusing on defending military computer networks, there appears to be no federally funded organization responsible for safeguarding the integrity of computer-controlled systems at the municipal level—where deployments and support operations are staged and controlled.

The ability to instill a sense of urgency in the actors on the information infrastructure is often impeded by the inability to share information. Many commercial interests are reluctant to report incidents to government agencies because they have no guarantee that sensitive information will be kept confidential—imagine a run on a bank by investors frightened away by a report that the bank was being harassed or forced to pay hacker ransom. Many companies are concerned they may lose control of trade secrets or proprietary information, or suffer unfair trade or antitrust investigation if the government is invited into their operations. As Harris Miller, president of the Information Technology Association of America, told the SafeNet 2000 infrastructure panel in December 2000, "The risks in reporting are clear: the fear of negative publicity, proprietary information shared in court, loss of public confidence or reduced trust in the economy itself." On the government side, much of the threat warning information on cyberterrorism and hacker investigations is considered classified and not to be disseminated

beyond certain very controlled groups, a sensitive concern with the proliferation of multinational corporations and companies with significant foreign ownership. [41]

Regarding local CND issues, the challenges are generally in the categories of either logical or physical protection. In most logical protection measures the first line of CND is the installation of a firewall. A firewall is a combination of hardware and software components that provide a controlled choke point between a "trusted" network (that of the organization) and an "untrusted" network, for example the Internet. The lack of security and discipline on the Internet has forced many corporations and agencies to install firewalls on their gateways to provide some control on what can come into their trusted network.

Briefly, a firewall consists of two common hardware components: the screening router and the application gateway, or "bastion" host. The screening router provides the primary connection between the trusted and untrusted networks. It routes IP data packets across the network interface and can be set up to block unwanted packets. Since many network applications now employ protocols that are too complicated for the router to handle, the second device, the application gateway, provides an extra layer of protection for these network applications. It can provide incoming Telnet or File Transfer Protocol (FTP) connections with one-time password authentication to prevent any unauthorized user from capturing and reusing the password to get into the trusted network at some other time.[42]

It is not as easy to deter the increasingly capable hacker with the firewall system, however robust it may be, as it was only a few years ago. In the November 2000 FedCIRC Newsletter, Director David Jarrell points out:

> there is a pervasive view among many Chief Executive Officer and Chief Information Officers that if one has good Information Technology (IT) perimeter security (e.g. firewalls) there is no need for [an Intrusion Detection System] IDS. No matter how well configured a firewall is, it will never stop all malicious or unauthorized traffic from outside the agency's IT perimeter, and it does not see

[41] Deborah Radcliff, "Inforwargames," *Computerworld*, 22 January 2001, 44.
[42] Stephen P. Cooper, *Internet Firewalls*, CIAC Notes 03, available from http://www.alw.nih.gov/Security/CIAC-Notes/CIAC-Notes-03.html; Internet, accessed 2/24/01.

> any network traffic inside the IT perimeter. IDS can monitor all network traffic that is allowed through the firewall from outside the IT perimeter towards systems inside the perimeter, all network traffic from inside the perimeter whose destination is outside the firewall and perimeter, and all network traffic between internal systems. This will allow the IDS to immediately alert all appropriate personnel to unauthorized and potentially malicious activity.[43]

Significant progress has been made recently in the design and function of Intrusion Detection Systems (IDS). There are two main classifications of IDSs. The first concerns which type of intrusion detection technique is employed, anomaly or misuse. The anomaly detection approach uses a set of statistical metrics that models the behavior of a user, group of users, or a host computer. The metrics could include mean duration of an FTP session, amount of data transmitted in each direction during a session, time of day of logons, etc. By constantly comparing current status to the metrics, the system can determine a deviation from normal and can signal an alarm to the system security officer. Setting the parameters for tripping the alarm is key to this technique, so the profiles need to be constantly updated. The misuse detection approach works by searching for a set of patterns from known attacks that have been stored in the system's database, patterns that occur every time such an attack occurs. An obvious difficulty with this setup is the need to constantly update the rule base as new attack methods become known.

The second classification of the IDS concerns whether it monitors activity on a single host and its subordinate terminals, or on multiple hosts interconnected by a network. The original IDSs examined audit data on a single host and based decisions solely on that information, making it impossible to detect attacks that were perpetrated by multiple sources or that spanned multiple machines in a network. They relied heavily on logs that an intruder could alter by either delaying their creation or deactivating the log routine altogether. The more efficient solution is to passively monitor the network for suspicious activity, using ubiquitous protocols that allow monitoring of heterogeneous networks independent of their architecture. By structuring IDSs in a

[43] David Jarrell, *The FedCIRC Bits & Bytes*, vol 1, issue 5, 1 November 2000.

cooperative layered architecture, each node using this model can operate more efficiently by aggregating the audit data it receives from the lower layers and passing a summarized form of the audit to the next higher layer. Intrusions can be detected at any layer, with the simpler ones most likely detected at the lower layers.[44]

Vigorous ongoing efforts to enhance computer network security capabilities have resulted in significant and important technological breakthroughs. Though certainly a most powerful tool for communications and electronic transactions, the topology of the Internet is such that it will never be regarded as a trusted network. Internet users cannot see or hear each other, may not even know each other, and therefore have little to verify the integrity of a message or to authenticate the identity of its originator. The latest word in user security is being hailed as a significant part of the answer to this challenge: Public Key Infrastructure (PKI).

Ciphers are used to substitute a block of text with another according to a predefined set of rules. The cipher is used in conjunction with a key to encrypt the message for the originator, and a key to decrypt the message at the receiving end. Symmetric ciphers use the same key at both ends, while asymmetric ciphers employ one key to encrypt the message and another to decrypt—a significant advantage when it comes to distribution and management of keys. PKI uses the asymmetric cipher method, with a publicly distributed key for encryption of messages to a particular addressee, and a private decryption key held only by that message addressee. Provided the addressee maintains the security of his private key, no other user can read messages enciphered by his public key.[45]

Briefly, the PKI system requires the originator to generate, in conjunction with his private key and a hash function, a set of text block checks, which are verified at the receiving end. If any of the checks from the originator do not match those decrypted by the receiver, then the message

---

[44] Panagiotis Astithas, *Intrusion Detection Systems*, Daemon News, May 1999, available from http://www.daemonnews.org/199905/ids.html; Internet, accessed 2/24/01.
[45] Julian Ashbourn, *Biometrics and PKI*, 2000, available from http://homepage.ntlworld.com/avanti/pki.htm; Internet, accessed 2/26/01.

has been tampered with and should be resent. The originator also creates a "digital signature" using his private key to create a unique identifier for the message, which is then decrypted at the receiving end and verified. When message encryption is used in conjunction with digital signatures within the PKI environment, the confidence in being able to securely transfer data over an untrusted network is increased tremendously. DoD is working toward establishing PKI through the use of a common access card system. Authorized users will carry their personal keys on the card and be able to gain access from virtually any terminal with network connectivity while retaining the ability to remove personal keys and thereby reduce the risk of compromise.

Though reduced, the risk remains of loss or compromise of PKI public or private keys, a risk that will hopefully be remedied through biometrics. Efforts in the area of biometrics are ongoing to devise a way for rapid verification of the identity of an individual accessing a computer terminal, the goal being to negate any gains from the compromise of passwords, personal identification numbers (PIN) or public/private keys. In response to the Army being designated Executive Agent for DoD biometrics,[46] LTG Cuviello announced the establishment of the Biometrics Management Office (BMO) in his September12, 2000, IA Conference speech. Biometrics is the use of physiological and/or behavioral characteristics to verify the identity of an individual. Some of the characteristics used include fingerprints, retinal and iris scanning, hand geometry, voice patterns, and facial recognition. Once the technology has matured it has the potential for tremendous impact in protecting the information infrastructure, from preventing misuse of corporate computer assets to thwarting enemy use of deployed military systems that are captured or overrun.[47]

However, even the most robust hardware and software protection mechanisms cannot provide complete CND. The dynamic nature of the threat to global networks and protection

[46] Deputy Secretary of Defense memorandum, dated 27 December 2000, Subject: Executive Agent for the Department of Defense (DoD) Biometrics Project. Available from http://www.biometrics.org/REPORTS/memo.pdf; Internet, accessed 2/27/01.
[47] Julian Ashbourn, *Biometric Whitepaper*, 1999, available at

systems, with new intrusion tools and malicious programs being developed constantly, requires persistent monitoring, detection, and implementation of system upgrades and software fixes. An alarmingly consistent trend is the lack of response by trusted agents, and even computer system administrators, to known computer system security vulnerabilities. In a message to all Army activities dated 16 January, 2001, LTG Keane, Vice Chief of Staff of the Army, says that in calendar year 2000 the Army reported fifty information system intrusions. Of these, eighty-eight percent were the result of "failures to implement identified fixes for known security vulnerabilities." He goes on to say that Army compliance verification team inspections of twenty-six organizations found nearly 800 instances of previously identified vulnerabilities still present on Army networks. Of most concern, however, is the fact that 730 of those instances were reported as having been corrected.

Disregarding the integrity issue, network security within DoD, as with all other corporate and public networks, is a community effort. The failure of any one node to maintain the security standard adversely affects all other nodes to which it is connected. As LTG Keane explains:

> Vulnerabilities on Army information systems represent a grave threat to the Army and the entire DoD due to the interconnected nature of DoD networks and our ever-increasing dependence on information processes, systems, and technologies. Would-be intruders have the tactical advantage—they pick the targets, conduct reconnaissance, and choose the time and method of execution to exploit our networks. Furthermore, the widespread availability of increasingly sophisticated network intrusion tools means that our networks are immediately exploited when a vulnerability is discovered.[48]

On the physical side of the security challenge is another issue of particular concern to computer security—the inside threat, or unauthorized access by authorized users. In testimony before the Senate Judiciary Committee on October 6, 1999, NIPC Director Michael Vatis cited the disgruntled insider as the principal source of computer crimes. His statement is all the more powerful when backed up by the January 2001 arrest of Robert P. Hanssen, Vatis' co-worker at

---

http://homepage.ntlworld.com/avanti/whitepaper.htm; Internet, accessed 2/26/01.

[48] Department of the Army (DACS-ZB) message, date-time group 160453Z Jan 01, Subject: Defense of Army Information Systems.

the FBI. On February 23, 2001, on the National Public Radio program *Morning Edition*, the imprisoned hacker Kevin Mitnik[49] was interviewed from jail regarding computer security. The program discussion centered on the point that a computer security system is only as good as it's weakest point, which more often than not is the authorized user. With the current proliferation of corporate operations into compartmented groups, there is a markedly lower degree of interpersonal contact between computer system users. The security of the system, regardless of the physical and logical protections installed (guard points, firewalls, IDS, etc.), can be easily circumvented through what Mitnik termed "social engineering," the deliberate duping of authorized users. Corporate employees, as trusted agents, are easily exploited as either malicious (in the case of those disgruntled with the company) or unwitting (naïve or inexperienced workers) accomplices in foiling security measures. Eager to help a caller, the employee is easily led to download data to a floppy disk and carry it undetected past the guard point. Or feigned trouble by a needy customer in receiving some faxed information can, with a little coaxing, yield the company's daily fax code allowing the caller to access the fax, and thus the entire system. Though effective if used as intended, PINs and passwords can be stolen, shared, or compromised through guessing or through the use of cracking software. An unauthorized user equipped with any one of these compromised keys has access to all the privileges of the authorized user. The bottom line is the need for a change in mindset when it comes to computer security—to suspect everyone first, and trust later.[50]

LTG Keane points out that for the Army, and by association for DoD, the issue is one of force protection and therefore a command concern. CND by necessity requires a defense in depth strategy, heavily reliant on effective defensive measures being implemented at the front line—at the local area network (LAN) and user level. The same point is made by the GAO in it's list of improvements needed to assure the security of federal computer operations:

[49] Kevin Mitnik was indicted in September 1996 for making unauthorized access to several corporate computer systems and copying proprietary software.

> . . . senior agency officials have not recognized that computer-supported operations are integral to carrying out their missions and that they can no longer relegate the security of these operations solely to low-level technical specialists. . . . there is a tendency to react to individual audit findings as they are reported, with little ongoing attention to the systemic causes of control weaknesses.[51]

A case in point regarding the timely implementation of published defensive measures is the recent announcement by the CERT/CC of a security gap in multiple versions of the Internet Software Consortium's Berkeley Internet Name Domain (BIND) server program. The BIND software allows the server to translate test-based Internet addresses into numbered IP addresses that are understood by computers. The vulnerability could enable unauthorized users to get control of the server and redirect or block requests sent to the server. The result could be a catastrophic remapping of major portions of the Internet. Though it is an older version of BIND that has the problem, it is estimated that approximately 80 percent of domain-name servers still use it. It is imperative that systems and network administrators apply security patches in a timely manner as they are published.[52]

With all the arguments for security actions, training, and manning of IA activities, the requirement to adequately resource these vital missions cannot be overlooked. Manpower caps within DoD restrict the ability to provide additional support and expertise to accomplish the previously unknown IA mission. The result is that many DoD personnel must perform vital IA tasks as additional duties, part time help providing the critical front line effort at securing the information infrastructure. Lack of training and experience in this critical field can be devastating, as pointed out by the FBI's list of ten most common security blunders by IT workers:

- connect systems to the Internet before hardening them
- connect test systems to the Internet with default accounts or passwords
- fail to update systems when security holes are found
- use Telnet and other unencrypted protocols for managing systems, routers, firewalls and public-key infrastructures

---

[50] National Public Radio's *Morning Edition*, "Computer Protection," 23 Feb 01.
[51] Congress, Senate, Committee on the Judiciary, Subcommittee on Technology, Terrorism and Government Information, *Critical Infrastructure Protection: Fundamental Improvements Needed to Assure Security of Federal Operations*, 6 October 1999, 4.
[52] Dan Verton, "Morning Update," *Computerworld*, 29 January 2001.

- give out passwords to users over the phone or change passwords without verifying the legitimacy of the request
- fail to maintain and test backups
- implement firewalls that don't stop malicious or dangerous traffic
- fail to update virus detection software
- fail to educate users about security problems
- allow untrained users to take responsibility for securing important systems.[53]

For many of the systems monitoring and responding to CND problems there is also a significant bandwidth requirement, adding overhead data to an already burdened transport system. For deployed military systems the limitation of bandwidth is especially acute, potentially restricting the use of many off-the-shelf IA products in tactical applications.

Finally, there are the legal challenges of CND. Efforts to be proactive and take on an actively defensive role have serious legal and political repercussions, as highlighted by the reaction of Japan to a recent incident. Hackers broke into official websites at two Japanese government agencies, left messages critical of the government, inserted unauthorized hyperlinks, and erased key data, including census figures. The London Daily Telegraph reports that, in response, the Japan Defense Agency is expected to deploy the "cyber squad" to design software capable of launching anti-hacking and anti-virus attacks.[54]

In the domestic arena, progress has been slow in revamping law to account for cybercrime. Despite the general adequacy of laws defining the substance of criminal and other offenses, significant legal challenges block effective law enforcement investigation. Changes are needed to allow real-time tracing of Internet communications across traditional jurisdictional boundaries (domestic and international) and close coordination among law enforcement agencies. In some instances, laws regarding evidence and procedure may need to be amended to allow for effective law enforcement.[55]

---

[53] Elinor Abreu, "FBI, DOJ Issue List of Worst Internet Threats," *The Industry Standard*, 1 June 2000.
[54] Juliet Hindell, "Japan Wages 'Cyber War' Against Hackers," *London Daily Telegraph*, 24 October 2000.
[55] *Report of the President's Working Group on Unlawful Conduct on the Internet*, (March 2000), available from http://www.usdoj.gov/criminal/cybercrime/unlawful.htm; Internet, accessed 2/27/01.

## CHAPTER 4

### Conclusions and Recommendations

> Two Kazakhstan citizens were arrested on August 10, 2000, in London, England for allegedly breaking into Bloomberg L.P.'s computer system in Manhattan in an attempt to extort money from Bloomberg. One sent e-mails to founder Michael Bloomberg demanding $200,000 in an offshore account in exchange for information on how the computer system was infiltrated. An account was set up in a London bank, the funds deposited, and a meeting arranged in London to resolve the issue. Two men showed to the meeting, reiterated the demands, and were promptly arrested after the meeting broke up.[56]
>
> A former chief network administrator was found guilty of unleashing a computer programming "timebomb" that deleted all design and production programs of a New Jersey-based high-tech measurement and control instruments manufacturer. The damage, lost contracts and lost productivity to the Omega Engineering Corp. of Bridgeport, N.J.—a manufacturing firm serving NASA, the Navy as well as private companies—totaled more than $10 million. The losses make it among the most expensive computer sabotage cases in the country. Two weeks after the perpetrator was fired, the timebomb was unleashed as planned, deleting and purging Omega's most critical manufacturing programs.[57]

The incidents cited reflect some of the difficult challenges in dealing with computer network attacks. They come from globally dispersed sites at the speed of light with no regard for international borders, often instigated by persons with trusted access to the very systems being attacked. The marked increase in the number and frequency of attacks has been accompanied by a steady acceleration in the complexity of the threat. David Barnes of Symantec's Anti-virus Research Center (SARC) estimates 50 percent of the increase in 32-bit worms and viruses occurred during the year 2000. He goes on to say that the proliferation of mobile devices

---

[56] Department of Justice, *News Release: Three* [sic] *Kazakh Men Arrested In London for Hacking Into Bloomberg L.P.'s Computer System*, by U.S. Attorney, Southern District of New York (14 August 2000). Bloomberg L.P., founded in 1981, is an information services, news, and media company serving customers in 100 countries. Headquartered in New York, it employs over 7,000 people in 9 sales offices, 2 data centers and 79 news bureaus worldwide (available from http://www.bloomberg.com/corp/press/bbglp.html; Internet, accessed 2/27/01).

[57] Department of Justice, "Former Computer Network Administrator Guilty of Unleashing $10 Million Programming 'Timebomb'," (9 May 2001), available from http://www.usdoj.gov/criminal/cybercrime/njtime.htm; Internet, accessed 2/26/01.

(handheld computers, mobile phones, etc.) indicates malicious code authors will soon target them as well. But Barnes goes on to postulate:

> These threats can be avoided or marginalised if the vendors of mobile computing and telephony devices rationalise the functionality, encapsulate features like scripting within the devices security model and enhance that security with digital signatures, encryption and access control. Only then will mobile computing remain safe computing.[58]

The recent DOS attacks that made Microsoft web sites inaccessible on three separate occasions were another wake up call to private industry that no one is immune and that all need to ensure full functionality of software security routines.[59]

The current status of CND efforts within DoD supports the conclusion that DoD can effectively implement timely and appropriate responses to detected computer network attacks. Though there remains room for improvements to DoD monitoring and detection capabilities, the positive progress and sense of urgency demonstrated by ongoing efforts forecasts a promising future. Important progress has been made in recent months in establishing among the nation's public and private sector leadership the sense that national security is directly tied to economic security which, in turn, is dependent on the viability and security of the national infrastructures. Based on the arguments and issues briefly discussed herein, and reflecting key elements of the National Plan for Information Systems Protection[60] (called the Plan hereafter), several conclusions can be drawn.

The process for disseminating information on computer network attacks is, except in the case of DoD, inadequately defined with too many advisory boards and groups dealing with the same issue and no entity apparently in charge. Alan Paller, member of the NIAC and director of the SANS Institute[61] in Bethesda, Maryland, says "The loose network of committees and councils

---

[58] David Barnes, "Looking Forward in 2001," *SARC AntiVirus Newsletter,* January 2001.
[59] Todd R. Weiss, "Microsoft Admits Defense Against Attacks Was Inadequate," *Computerworld,* 29 January 2001.
[60] The White House, "National Plan for Information Systems Protection Version 1.0," (Washington, D.C.).
[61] The System Administration, Networking, and Security (SANS) Institute, founded in 1989, is a cooperative research and education organization through which more than 96,000 system administrators,

have not yet had a positive impact and I have not heard any arguments that would lead me to believe the impact will improve. . . . it is a basic mismatch that occurs when you ask well-meaning non-technical people to guide the actions needed to solve a thorny technical problem."[62] Richard Clarke, chief orchestrator of the Plan as National Coordinator for Security, Infrastructure Protection, and Counter-Terrorism, admits the Plan is not laid out in great detail. In his forward remarks he says the Federal government will help private sector groups as they commit to uniting and defending their computer networks, but the government will not dictate solutions or regulate their actions.

The DoD structure for CND is clear in that all reports flow up, and are shared as appropriate throughout, an unambiguous chain of IA centers to the JTF-CND. The JTF-CND then provides command response direction with mandatory compliance by all DoD elements. The ongoing formation of private sector ISACs is certainly encouraging and indicative of a growing sense of cooperation and interdependence, but until a Federal hierarchy is established for reporting detection of attacks and authoritatively directing coordinated responses, the current situation of confusion and lack of trust will prevail. Direction would not have to be binding, but there needs to be one government source of sanctioned information and direction. Though the government has no ownership and limited jurisdiction of the infrastructure, a clear federal strategy is needed to assert better control of federal department and agency use of the infrastructure. With network access only as effective as the weakest node or user, protection of the vital information infrastructure deserves better government direction.

---

security professionals, and network administrators share the lessons they are learning and find solutions for challenges they face. The core of the institute is the many security practitioners in government agencies, corporations, and universities around the world who invest hundreds of hours each year in research and teaching to help the entire SANS community. During 2000 and 2001, this core will grow rapidly as the Global Incident Analysis Center and the GIAC Certification programs develop mentors who will help new security practitioners master the basics.

[62] Dan Verton, "Clinton Makes Last-minute Cybersecurity Appointments," *Computerworld*, 22 January 2001.

Federal government efforts and direction should reach out to lower level governments, providing for protection of national security down to the municipal level where DoD deployment and sustainment issues are affected. Extending the argument to the international arena, the United States government should lead the way in demonstrating decisive response to global information threats through installation of robust security measures on U.S. government assets and through conduct of openly cooperative efforts to deal with cross-border attacks. Progress must be made toward determining a global hierarchy with authority to orchestrate international CND efforts—the global economy can ill afford repetition of the Internet shutdown problems incurred by the "I Love You" virus.

A way must be found to support government elements charged with protection of private industry's capability of sharing and being able to share CND information in a timely manner (e.g. NIPC), while protecting sensitive proprietary data and fostering trust and confidence in the private sector. Success should strengthen public sector support for the reporting process, and hopefully create in the private sector the ethical sense of duty to protect the rights of citizens to secure banks and unaltered medical records. The government should help the private sector realize how much money their information and organizational reputations are worth when it comes to investing in and supporting IA activities. Installation of available protection measures to known attack threats must continue to be encouraged in the strongest sense—for DoD elements, non-compliance could possibly be dealt with by denial of access.

Government network servers should set the standard for firewall and IDS protection and timely implementation of all software security updates. Reliance on hardware systems alone for CND is unsound; no hardware protection is completely successful. Therefore, research and development investments must continue, especially in the areas in PKI and biometrics which are potentially effective means for reducing the inside threat. Investments in education of information system subscribers must also continue and be encouraged in the private sector, to enable users to employ the computer network media intelligently and not be duped into

inadvertently aiding unauthorized access. As trusted network agents that store, process and transfer the most sensitive government information, DoD systems administrators and key IA personnel should be given security background checks.

IA activities must be adequately resourced, not treated as additional duties. Hardware and software system installations must take advantage of the latest technological advances in security and CND protection. Personnel entrusted with managing the information infrastructure must be trained and certified. In addition to maintaining the DoD training programs already in effect, and as suggested in the Plan, scholarships could be used as an aid in recruiting the next generation of IT workers—funding college students in IT programs in exchange for future service along with summer work and internships. Promising high school students could be included in summer-hire programs that could result in IT certifications and future employment.

Immediate action is needed to remedy legislative issues constraining effective CND. To facilitate further growth of the ISAC organizations and promote private sector incident reporting, the government must seek ways to ensure its ability to protect sensitive information and allay potential liability and antitrust concerns associated with sharing such information by and with the private sector (e.g. Freedom of Information Act). Action must be taken to empower law enforcement agencies to conduct real-time tracing of Internet communications across traditional jurisdictional boundaries, both domestically and internationally. Work must continue to establish legal procedures that effectively coordinate federal, state, local and global authorities in gathering evidence, conducting investigations, and prosecuting cases. Procedural and evidentiary laws may have to be amended to enable law enforcement to meet the challenge. In all these efforts the overarching need to protect the civil liberties and privacy of U.S. citizens must be kept in mind.

## APPENDIX A
### Glossary of Acronyms

ACERT—Army Computer Emergency Response Team (DoD)

AFCERT—Air Force Computer Emergency Response Team (DoD)

ARPANET—Advanced Research Project Agency Network

BIND—Berkeley Internet Domain Name

BMO—Biometrics Management Office (DoD, Department of the Army, DISC4)

C4—command, control, communications and computers

C4IFTW—Command, control , communications, computers and intelligence for the warrior

CD—compact disk

CERT/CC—Computer Emergency Response Team/Coordination Center

CIAC—Computer Incident Advisory Capability (DoE)

CIAO—Critical Infrastructure Assurance Office (Department of Commerce)

CICG—Critical Infrastructure Coordination Group

CID—Criminal Investigation Division (DoD, Army)

CINC—Command in Chief (DoD)

CINCPAC—Commander in Chief, Pacific (DoD)

CINCSPACE—Commander in Chief, U.S. Space Command (DoD)

CIO—Chief Information Officer

CJCS—Chairman, Joint Chiefs of Staff (DoD)

CNA—computer network attack

CND—computer network defense

CONUS—continental United States

COP—Common Operational Picture

DA—Department of the Army

DII—Defense Information Infrastructure

DISA—Defense Information Systems Agency (DoD)

DISC4—Director of Information Systems for Command, Control, Communications and Computers (DoD, Department of the Army)

DITY VAP—Do-it-yourself Vulnerability Assessment Program (DoD, ACERT)

DMS—Defense Message System (DoD)

DoD—Department of Defense

DoD-CERT—Department of Defense Computer Emergency Response Team

DoDD—Department of Defense Directive (DoD)

DoE—Department of Energy

DOS—denial-of-service attack

DRSN—Defense Red Switch Network (DoD)

FedCIRC—Federal Computer Incident Response Center

FBI—Federal Bureau of Investigation

FTP—File Transfer Protocol

GNOSC—Global Network Operations and Security Center (DoD, DISA)

GSA—General Services Administration

IA—information assurance

IAVA—Information Assurance Vulnerability Alert (DoD)

IAVB—Information Assurance Vulnerability Bulletin (DoD)

IDS—intrusion detection system

INFOCON—Information Operations Condition

INMS—Internet Network Management System

IO—information operations

IP—Internet protocol

IPMO—Information Assurance Program Management Office (DoD, DISA)

ISAC—Information Sharing and Analysis Center

IT—information technology

JTF-CND—Joint Task Force for Computer Network Defense (DoD, USSPACECOM)

LAN—local area network

LCC—Local Control Center

LEA—law enforcement agencies

MTT—Mobile Training Team

NATO—North Atlantic Treaty Organization

NAVCIRT—Navy Computer Incident Response Team (DoD)

NIAC—National Infrastructure Assurance Council

NIPCI—National Infrastructure Protection and Computer Intrusion element (FBI)

NIPRNET—Non-secure Internet Protocol Router Network (DoD)

NIPC—National Infrastructure Protection Center (FBI)

NSA—National Security Agency

NSC—National Security Council

OCIP—Office of Critical Infrastructure Protection

OMB—Office of Management and Budget

PDD—Presidential Decision Directive

PKI—Public Key Infrastructure

PIN—personal identification number

RNOSC—Regional Network Operations and Security Center (DoD, DISA)

SAIC—Science Applications International Corporation

SARC—Symantec Anti-virus Research Center (corporate enterprise)

SIPRNET—Secure Internet Protocol Router Network (DoD)

SRI—Stanford Research International

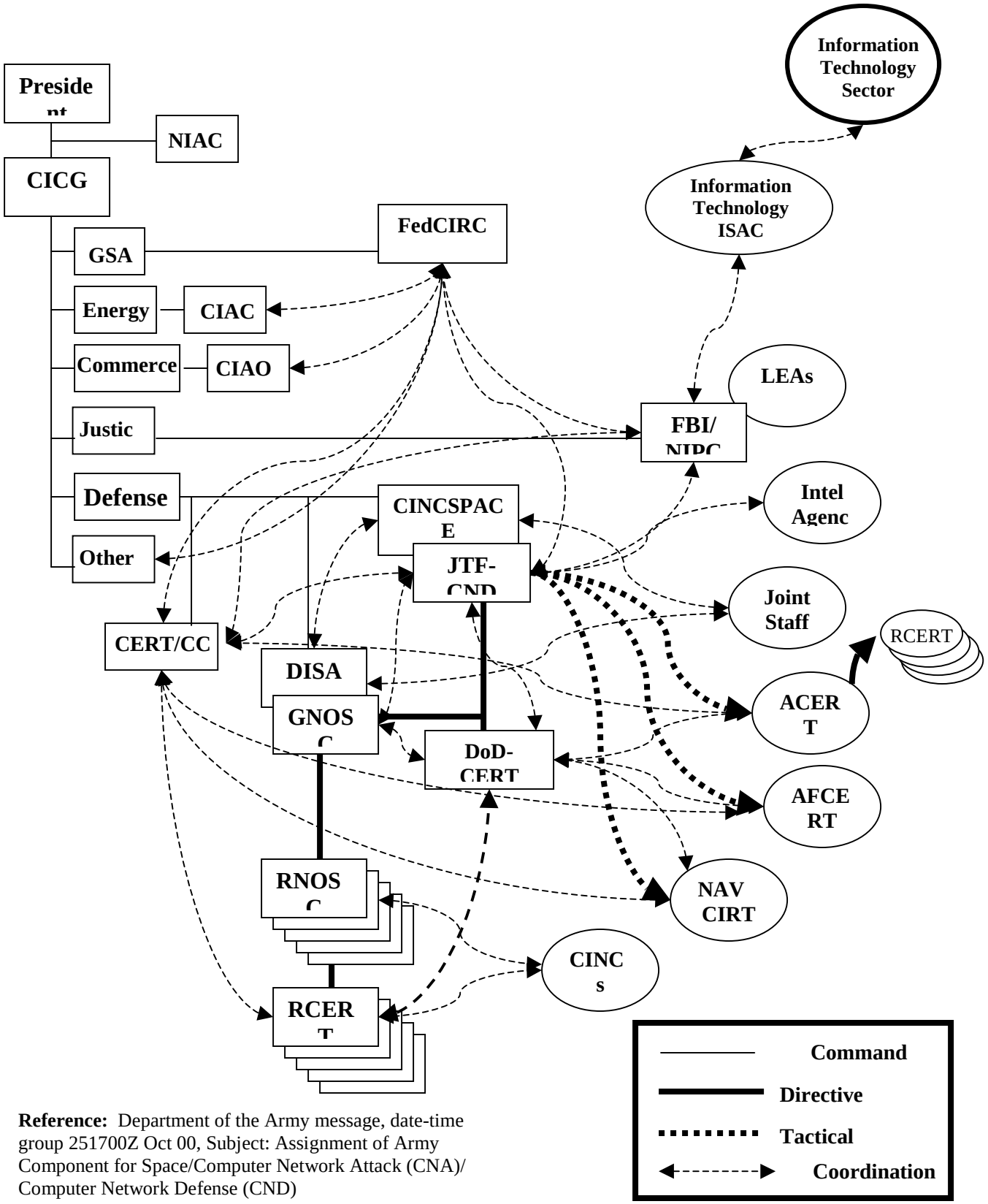
STU-III—Secure Telephone Unit, third generation

TMS—Trouble Management System

Y2K—year 2000

**APPENDIX B**

# Computer Emergency Response Community




**Reference:** Department of the Army message, date-time group 251700Z Oct 00, Subject: Assignment of Army Component for Space/Computer Network Attack (CNA)/ Computer Network Defense (CND)

## BIBLIOGRAPHY


Abreu, Elinor. "FBI, DOJ Issue List of Worst Internet Threats." *The Industry Standard*, 1 June 2000.

Angelica, Amara D. "The New Face of War." *Techweek*, 2 November 1998.

Arquilla, John and David Ronfeldt. *In Athenas Camp*. Santa Monica, CA: RAND National Defense Research Institute, 1997.

Ashbourn, Julian. "Biometrics and PKI." *Avanti Biometric Reference Site*. Available from http://homepage.ntlworld.com/avanti/pki.htm; Internet, accessed 2/26/01.

_____. "Biometric Whitepaper." *Avanti*, 1999. Available at http://homepage.ntlworld.com/avanti/whitepaper.htm; Internet, accessed 2/26/01.

Astithas, Panagiotis. "Intrusion Detection Systems."*Daemon News*, May 1999.

Barnes, David. "Looking Forward in 2001." *SARC AntiVirus Newsletter*, January 2001.

Carnegie Mellon Software Engineering Institute. *CERT/CC Statistics 1988-2000*. Available from http://www.cert.org/stats/cert_stats/html; Internet, accessed 2/24/01.

Cooper, Stephen P. "Internet Firewalls." *CIAC Notes*, 03. Available from http://www.alw.nih.gov/Security/CIAC-Notes/CIAC-Notes-03.html; Internet, accessed 2/24/01.

Cuviello, Peter M., LTG. *Information Assurance Readiness Review and IA Force Protection Program* Assessment. Speech delivered to the Information Assurance Conference on 12 September 2000 in Crystal City, VA.

Defense Information Systems Agency. *DISA Network Incident Reporting Guidelines*. Available from http://www.cert.mil/pub/info/general/network.security/reportguidelines/pdf; Internet, accessed 02/22/01.

Denning, Dorthy E. "Cyberterrorism." Testimony before the U.S. House of Representatives Special Oversight Panel on Terrorism Committee on Armed Services. Washington, D.C., 23 May 2000.

Dolak, John. *DITY VAP*. Electronic mail, 24 January 2001.

Green, Stephen. "Pentagon, Once Stung, Beefs Up Cyberwarfare Role." *Copely News Service*, December 24, 1999.

Hindell, Juliet. "Japan Wages 'Cyber War' Against Hackers." *London Daily Telegraph*, 24 October 2000.

Jarrell, David. "Waling a Technical Tightrope." *The FedCIRC Bits & Bytes*, vol 1, issue 5, 1 November 2000.

Lew, Jack. *Guidance on Implementing the Government Information Security Reform Act*. Office of Management and Budget memorandum dated 16 January 2001

Liang, Qiao and Wang Xiangsui, *Unrestricted Warfare*. Beijing: PLA Literature and Arts Publishing House, 1999.

*Morning Edition*. "Computer Protection." Host Bob Edwards. National Public Radio. KCUR. Kansas City. 23 Feb 01.

Radcliff, Deborah. "Inforwargames," *Computerworld*, January 22, 2001.

*Report of the President's Commission on Critical Infrastructure Protection*. By Robert T. Marsh, chairman. Washington, D.C.: Government Printing Office, 1997.

*Report of the President's Working Group on Unlawful Conduct on the Internet*. Washington, D.C.: Government Printing Office, 2000.

Roos, John. "USSPACECOM Readies For Computer Network Attack Mission." *Armed Forces Journal International*, 2 October 2000.

"Statistics on Cyber-terrorism," available from http://www-cs.etsu.edu/gotterbarn/stdntppr/stats.htm; Internet; accessed 1-/25/2000.

The White House, *A National Security Strategy for a New Century*. Washington, D.C., 1998.

_____. *National Plan for Information Systems Protection Version 1.0*. Washington, D.C.: Government Printing Office, 2000.

_____. *PDD63: White Paper on Administration's Policy on Critical Infrastructure Protection*. Office of the Press Secretary, May 1998. Available from http://www.ciao.gov/CIAO_Document_Library/paper598.pdf; Internet, accessed 25/10/00.

_____. *White Paper: Protecting America's Critical Infrastructures, PDD-63*. Office of the Press Secretary, May 22, 1998. Available from http://www.info-sec.com/ciao/63factsheet.html; Internet, accessed 25/10/00.

Turabian, Kate L. *A Manual for Writers of Term Papers, Theses, and Dissertations*. 6th ed. Chicago: University of Chicago Press, 1987.

U.S. Army Computer Emergency Response Team. *Procedures for Incident/Intrusion Handling*. Electronic mail attachment from Richard Simon, Director, Land Information Warfare Agency Detachment, Fort Leavenworth, KS.. 16 February 2001.

U.S. Congress. Senate. Committee on the Judiciary, Subcommittee on Technology, Terrorism and Government Information. *Critical Infrastructure Protection: Fundamental Improvements Needed to Assure Security of Federal Operations*. 6 October 1999.

U.S. Department of the Army. “New Information Assurance (IA) Personnel Structure.” SAIS-IAS message DTG 020919Z Jun 00.

_____. “Defense of Army Information Systems.” DACS-ZB message DTG 160453Z Jan 01.

U.S. Department of Defense. *DoD Directive O-8530.1 Computer Network Defense (CND).* Washington, D.C., 2001.

_____. “Executive Agent for the Department of Defense (DoD) Biometrics Project.” Deputy Secretary of Defense memorandum. Washington, D.C., 27 December 2000.

_____. “Review of Revised DoD Information Operations Condition (INFOCON) Sytem Procedures.” USDEPCINCSPACE message DTG 012106Z FEB 01.

U.S. Department of Energy. *Critical Infrastructure Protection Program Related to Cyber Protection*. Washington, D.C., 1999.

U.S. Department of Justice, ”Former Computer Network Administrator Guilty of Unleashing $10 Million Programming ‘Timebomb’.” 9 May 2001.

_____. “News Release: Three [sic] Kazakh Men Arrested In London for Hacking Into Bloomberg L.P.’s Computer System.” By U.S. Attorney, Southern District of New York, 14 August 2000.

“U.S. Launches Cybercrime Web Site.” *Reuters*, 3 October 2000

U.S. President, Executive Order 13130. “National Infrastructure Assurance Council.” Available at http://cio.gov/docs/eo13130.htm; Internet, accessed 1/25/01.

Vatis, Michael A. “NIPC Cyber Threat Assessment, October 1999.” Statement before the Senate Judiciary Committee Subcommittee on Technology and Terrorism. Washington, D.C., 6 October 1999.

Verton, Dan. “Bush Eyes Overhaul of Nation’s E-security.” *Computerworld*, 19 December 2000.

_____. “Clinton makes last-minute cybersecurity appointments.” *Computerworld*, 22 January 2001.

_____. “Morning Update,” *Computerworld*, 29 January 2001.

Weiss, Todd R. “Microsoft Admits Defense Against Attacks Was Inadequate.” *Computerworld*, 29 January 2001.